UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	Civil Action No. 23-cv-9518-PAE

BRIEF OF BSA | THE SOFTWARE ALLIANCE AS AMICUS CURIAE SUPPORTING DEFENDANTS' MOTION TO DISMISS

James M. Garland (*pro hac vice* pending)
Megan A. Crowley (*pro hac vice* pending)
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
(202) 662-6000
jgarland@cov.com
mcrowley@cov.com

S. Conrad Scott
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018
(212) 841-1249
cscott@cov.com

Counsel for Amicus Curiae BSA | The Software Alliance

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Regulations, Guidance, and Policy Statements

Other Authorities

INTRODUCTION

In 2019 and 2020, Defendant SolarWinds Corporation experienced a nation-state attack that was "one of the worst cybersecurity incidents in history."[1] In a cyberattack of previously unseen scope and sophistication—subsequently dubbed "SUNBURST"—the Russian Foreign Intelligence Service infiltrated SolarWinds' Orion network-monitoring software and gained access to the systems of SolarWinds clients, including several U.S. government agencies.

Three years later, the U.S. Securities and Exchange Commission ("SEC") now accuses SolarWinds—the victim of that nation-state attack—and its Chief Information Security Officer ("CISO") of securities fraud. The SEC acknowledges that SolarWinds warned investors that it was vulnerable to cyber-threats and, within two days of learning about the intrusion, filed a Form 8-K in which it publicly disclosed that it had been the victim of a potentially massive cyberattack. Nonetheless, the SEC accuses SolarWinds of defrauding investors by not publicly disclosing details about its cybersecurity vulnerabilities or exactly how many customers were infiltrated through the SUNBURST attack. In support of its claims, the SEC points mostly to excerpts of communications among SolarWinds engineers and other employees who were working on cybersecurity issues.

This case is unprecedented. Never before has the SEC sued the victim of a nation-state cyberattack; sued a company for securities fraud based on the company's cybersecurity disclosures; or sought to hold an individual personally liable for those disclosures. This case is not only novel, but also threatens to undermine cybersecurity by making it more difficult for companies to respond to increasingly sophisticated and highly-resourced cyber-threats. To

[1] Compl. ¶ 11. No party's counsel authored this brief in whole or in part. No party, party's counsel, or any other person besides amicus, its members, or its counsel contributed money that was intended to fund the preparation or submission of this brief.

effectively manage cyber-risks and respond to attacks, companies must encourage employees to flag potential vulnerabilities—to "say something if they see something"—even if they might be wrong. They must sift through cyber-threats, actual and potential, and quickly decide how to respond, often without the benefit of full information. And if their systems are infiltrated, they must work closely with the government and oftentimes other companies to identify, contain, and remediate the threat.

If public companies must now fear the SEC will comb through their communications for evidence purporting to show that some of their employees were aware of undisclosed vulnerabilities, as the SEC has sought to do in this case, candid internal deliberations will be chilled and communications with law enforcement and national security authorities, other companies, and the public will be stifled, even though those communications are essential to effective cyber-defense. Moreover, requiring companies to publicly disclose details about cybersecurity weaknesses and incidents, as the SEC seeks to do here, will serve only to give threat actors more information about how better to attack American companies. Even the SEC has explicitly acknowledged this risk.

The theories of liability pursued in this case, against a nation-state victim and individual CISO, will undermine companies' ability to defend against cyber-threats, threatening our national security and leaving us all less safe. The Court should grant Defendants' motion to dismiss.

INTEREST OF AMICI

BSA | The Software Alliance is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth

in the digital economy. It and its members have strong interests in cybersecurity and therefore this case, which threatens to undermine global cybersecurity efforts.

Cybersecurity is more important than ever. Software innovation continues to connect people across the world and transform daily business practices.[2] These online connections create efficiencies and spur economic growth, but they also create vulnerabilities that bad actors, especially advanced persistent threats funded by nation-states, can exploit. In today's increasingly interconnected digital ecosystem, a single data breach can expose hundreds of millions of individuals' personal data.[3] As the SUNBURST attack aptly illustrates, the compromise of one company can allow threat actors to gain unauthorized access to the systems of many others, no matter how vigilant they are.

Cybersecurity is also more challenging than ever. Well-funded and technologically advanced adversaries are making increasingly sophisticated efforts to find and exploit cyber defenses. While organized criminal networks seek to profit from stealing personal information or holding businesses' data for ransom,[4] hostile nation-state actors and state-supported groups have turned to cyberattacks to gather intelligence, penetrate critical infrastructure and supply chains, and undermine confidence in public institutions. For example, Russian state actors have been persistent in their efforts to disrupt Ukrainian communications networks and to gather information on Ukraine's NATO allies.[5] In recent weeks, Taiwan has "face[d] a deluge of cyberattacks just

---

[2] BSA, *Policy Issues: Cybersecurity*, https://perma.cc/XCT2-D7SP; *see also* BSA, *Cybersecurity for the Connected Age*, https://perma.cc/FU7G-553J.

[3] Seena Gressin, FTC, Consumer Alert: The Marriott Data Breach (Dec. 4, 2018), https://perma.cc/PE4L-9NKA.

[4] *See, e.g.*, Dep't of Justice, Press Release, *U.S. Department of Justice Disrupts Hive Ransomware Variant* (Jan. 26, 2023), https://perma.cc/S7F8-QSCP.

[5] Grace B. Muller et al., Ctr. for Strategic & Int'l Studies, *Cyber Operations During the Russo-Ukrainian War* (July 2023), https://perma.cc/ZN5W-CPNP.

before a critical presidential election."[6] And nation-state actors have directed an increasing number of attacks at critical infrastructure, such as power grids, water systems, and healthcare facilities, attacks that pose grave risks to public safety and stand to cause significant civil and economic disruption.[7] Indeed, this case arises from just such an attack, which Russia's Foreign Intelligence Service staged to infiltrate several U.S. government agencies. (Although the SEC alleges that "certain reports" have attributed the SUNBURST attack at issue in this case "to a Nation-State actor,"[8] the Executive Branch has unequivocally attributed the attack to the Russian Foreign Intelligence Service.[9])

Combating these threats is a top priority for BSA. BSA supports efforts to improve the capabilities and readiness of governments and industries to address cybersecurity threats. These efforts include promoting a secure software ecosystem, strengthening cybersecurity workforce capabilities, supporting policies that enable the development of cutting-edge cybersecurity technologies, and taking other steps to secure and defend information infrastructure. For their part,

---

[6] Maggie Miller & Joseph Gedeon, *Taiwan Bombarded with Cyberattacks Ahead of Election*, Politico (Jan. 11, 2024), https://perma.cc/E6GU-24EE.

[7] *See, e.g.*, Aamer Madhani, *Top White House Cyber Aide Says Recent Iran Hack on Water System Is Call To Tighten Cybersecurity*, AP News (Dec. 8, 2023), https://perma.cc/4NSR-PFE4 (discussing recent cyberattacks carried out by hackers backed by Iran's Islamic Revolutionary Guards Corps, which "breached multiple organizations in several states including a small municipal water authority"); Ellen Nakashima & Joseph Menn, *China's Cyber Army Is Invading Critical U.S. Services*, Wash. Post (Dec. 11, 2023), https://perma.cc/RBA2-X6FK (discussing "Volt Typhoon" cyberattacks carried out by groups backed by China's People's Liberation Army on infrastructure targets including "a water utility in Hawaii, a major West Coast port and at least one oil and gas pipeline"); *see also* Cybersecurity & Infrastructure Sec. Agency ("CISA"), Cybersecurity Advisory: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection (May 24, 2023), https://perma.cc/58EQ-6ZYU.

[8] Compl. ¶ 144.

[9] *See, e.g.*, White House, Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government (Apr. 15, 2021), https://perma.cc/J3Q5-HHPQ; CISA, Cybersecurity Advisory: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations (Apr. 15, 2021), https://perma.cc/QQR8-SDYM.

BSA members and other companies have invested substantial resources in securing themselves and their customers against today's constantly evolving cybersecurity threats and, collectively, constitute the frontline defenses against them. These companies offer software and services that promote trust and security across cloud computing, customer relationship management, human resources management, and identity and access management.[10] Moreover, many of these companies have unparalleled visibility across thousands of networks and millions of endpoints globally, and they use that visibility daily to help their customers, the government, and the general public identify, protect against, detect, respond to, and recover from cyber-threats.

BSA submits that this unprecedented case will undermine cybersecurity and—at a time when clarity is urgently needed—sow confusion about how companies should disclose cybersecurity risks and incidents. BSA respectfully urges the Court to consider these risks as it decides Defendants' motion to dismiss.

ARGUMENT: THIS CASE THREATENS TO UNDERMINE CYBERSECURITY

I. This Case Will Hamper Companies' Ability To Effectively Remediate Cybersecurity Vulnerabilities and Respond to Unfolding Incidents.

In its complaint, the SEC advances an aggressive and expansive theory about how much information about cybersecurity vulnerabilities and incidents companies are required to disclose to their investors. As Defendants' motion to dismiss explains (at 3–6), SolarWinds disclosed to its investors that it was vulnerable to cyberattack, and, on learning about the SUNBURST attack, promptly disclosed to investors that it had been targeted in what was likely a "highly sophisticated, targeted and manual supply chain attack by an outside nation state" that could have affected up to

[10] *See* Letter from BSA to Vanessa A. Countryman, Sec'y, SEC, Regarding Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure 1 (May 9, 2022), https://perma.cc/5JXK-T7H6 ("BSA Comment Letter").

18,000 customers accounting for half the company's revenue. The SEC claims, however, that Defendants nevertheless defrauded investors because the company did not disclose particular cybersecurity vulnerabilities of which certain company employees were aware,[11] purported red flags signaling that the company was being targeted in a cyberattack,[12] or that there were allegedly reasons to believe that the SUNBURST threat actors had exploited those vulnerabilities to gain access to specific customers.[13] In effect, the SEC faults Defendants for the fact that the company did not publicly disclose specific cybersecurity vulnerabilities or that it was (allegedly) *especially* vulnerable to cyberattack, and because it did not *immediately* apprise investors of *specific* details about the SUNBURST attack.

If the SEC succeeds in holding Defendants liable for securities fraud based on that ambitious theory, other companies will take note. To avoid incurring securities-fraud liability themselves, companies will feel pressured to disclose information about their cybersecurity vulnerabilities and incidents too quickly and in excessive detail. Such disclosure is unlikely to be helpful for investors, who will be flooded with difficult-to-digest and likely immaterial information. Moreover, such disclosure will directly undermine cybersecurity in at least two ways.

First, by providing detailed disclosure about specific vulnerabilities, companies will effectively invite future attacks. Given the complexity and ubiquity of modern digital technology, it is inevitable that software and networks will contain weak points. The software industry works diligently to find and remediate these vulnerabilities before they are exploited, and software

[11] *E.g.*, Compl. ¶¶ 91–100 (allegations that SolarWinds gave too many employees "administrator" access); *id.* ¶¶ 102–10 (allegations that one software engineer thought that SolarWinds' VPN settings were "not very secure" and that SolarWinds did not correct these issues).

[12] *See id.* ¶¶ 145, 148–51, 153–64, 171.

[13] *See id.* ¶¶ 187–89; *see also id.* ¶¶ 101, 111, 132–34, 137, 151, 164.

companies routinely issue patches and updates for their products to address these problems.[14] The industry has developed principles and internationally recognized standards for Coordinated Vulnerability Disclosure—known as "CVD"—under which responsible actors who identify vulnerabilities can disclose them to government authorities and software vendors confidentially, giving software companies the opportunity to correct vulnerabilities before their existence becomes widely known.[15] The CVD process exists because indiscriminate public disclosure of a particular vulnerability, or even public awareness that a particular company or product has a serious vulnerability, before that vulnerability is remediated risks alerting malicious actors and providing a blueprint for future attacks.[16] Indeed, the SEC has explicitly acknowledged that requiring companies to disclose too much information about their cybersecurity vulnerabilities—especially before those vulnerabilities are fully remediated—risks making companies more vulnerable to future attacks.[17] Yet the theories advanced by the SEC in this case risk forcing companies to make this very kind of counterproductive and potentially dangerous disclosure.

Second, if companies are forced to make premature or overly specific disclosure about ongoing cyberattacks, those disclosures will impede efforts to mitigate those attacks. If, to minimize its potential SEC liability, a company races to disclose details about a newly detected ongoing incident, hackers may respond by accelerating the attack, exfiltrating sensitive information, covering their tracks, or taking other action that impedes ongoing incident-response efforts and identification of those responsible.[18] The potentially harmful effects of such premature

[14] *See* BSA Comment Letter at 8–9.

[15] *See* CISA, *Coordinated Vulnerability Disclosure Process*, https://perma.cc/R76B-D22V.

[16] BSA Comment Letter at 9.

[17] Final Rule, 88 Fed. Reg. 51896, 51911–12 (Aug. 4, 2023).

[18] BSA Comment Letter at 4.

disclosure are "innumerable."[19] Moreover, there is a risk that, in their haste to disclose detailed information about incidents as soon as incidents are discovered, companies will inadvertently provide investors with information that upon further investigation turns out to have been inaccurate or incomplete. Premature disclosure of details about cybersecurity incidents thus stands to benefit threat actors and create liability traps for companies without meaningfully benefitting investors.

At a minimum, the SEC's approach in this case has created significant uncertainty about companies' cybersecurity disclosure obligations. For example, the SEC has repeatedly told companies that they need not provide overly detailed disclosure about cybersecurity risks or incidents. In 2018, the Commission issued interpretive guidance that expressly disclaimed "suggest[ing] that a company should make detailed disclosures that could compromise its cybersecurity efforts—for example, by providing a 'roadmap' to those who seek to penetrate a company's security protections."[20]

In the last two years (well after the events at issue in this case), the Commission set out to codify that guidance in binding rules that standardize the disclosures public companies must make about cybersecurity risk management, strategy, governance, and incidents. The SEC initially criticized prevailing cybersecurity practices for providing "insufficient detail" and proposed requiring companies to reveal a trove of data about cyber incidents, including details about the scope of those incidents.[21] Facing widespread opposition to its proposed requirement,[22] the SEC reconsidered, adopting a Final Rule that "narrow[ed] the amount of information required to be

[19] *Id.* at 4. Again, the SEC has expressly acknowledged this risk. *See* 88 Fed. Reg. at 51903.

[20] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, 8169 (Feb. 26, 2018).

[21] Proposed Rule, 87 Fed. Reg. 16590, 16594, 16623 (Mar. 23, 2022).

[22] *E.g.*, BSA Comment Letter at 4–6.

disclosed."[23] Likewise, in response to commenters' criticisms of the accelerated timeframe for disclosure initially proposed by the SEC, the SEC acknowledged in the Final Rule that companies need time to investigate incidents and must be permitted to make modest, initial disclosures based on available information, which can be updated after further investigation.[24]

In this case, however, the SEC has reverted to a maximalist position about companies' cybersecurity disclosure obligations, advancing theories that run contrary to the policies it purported to adopt in its own recent rulemaking.[25] As a result, companies are left to guess about the level of detail they are actually required to provide when disclosing cybersecurity incidents and vulnerabilities: the more general level authorized by the Final Rule or the specificity the SEC's complaint seems to demand.

That uncertainty is doubly concerning. *First*, while companies are entitled to "fair notice … of the conduct that will subject [them] to punishment,"[26] such fair notice is lacking here, where companies must simply guess about the particularity of disclosures that will satisfy the SEC. *Second*, the SEC's attempt to impose higher standards through this case defeats the purpose of its own cybersecurity rulemaking. The SEC adopted a certain set of disclosure obligations through the notice-and-comment rulemaking process, yet now attempts to impose more demanding

---

[23] 88 Fed. Reg. at 51903.

[24] *See id.* at 51908.

[25] *Compare, e.g.*, *id.* at 51903, 51934, 51937 (requiring only "streamlin[ed]" disclosures about cybersecurity incidents), *with* Compl. ¶¶ 186–89 (faulting SolarWinds for its allegedly general and conditional disclosures of SUNBURST attack). Similarly, the SEC initially proposed requiring companies to disclose individually immaterial cyber incidents if those incidents became material in the aggregate, *see* 87 Fed. Reg. at 16599, 16619–20, 16624, then dropped that aggregation requirement in the Final Rule, 88 Fed. Reg. at 51903, 51910, only to apparently revive that theory in this case, Compl. ¶ 46 (even if individual incidents were immaterial, "[t]ogether, the individual failures, risks, issues, and incidents" had a material "collective effect").

[26] *BMW of N. Am. v. Gore*, 517 U.S. 559, 574 (1996).

obligations through litigation. The Court should not countenance the SEC's attempt to regulate via enforcement action.

II. This Case Endangers Companies' Ability To Communicate About Cybersecurity Issues.

This case also threatens to undermine cybersecurity by chilling open communications about cybersecurity issues between and among companies, government authorities, and the public at large. Cybersecurity requires effective cooperation among all responsible stakeholders. But by signaling that candid communications about cybersecurity issues may increase companies' exposure to SEC enforcement actions and private securities litigation, this case will discourage that cooperation—again, with the result of leaving us all less safe.

A. This Case Will Discourage Companies from Sharing Information with Law Enforcement and National Security Authorities and with Other Companies.

Cybersecurity relies on close cooperation between law enforcement and national security authorities and the private sector.[27] Unlike traditional threats to national security, "[c]yber is the sole arena where private companies are the front line of defense."[28] Private companies play a key role in keeping networks and users safe against cyberattack. As noted, many of these companies make substantial investments to strengthen their cybersecurity capabilities and keep their customers secure. When they or their customers are targeted by malicious activity online, they may have unique insights into the sources and methods used by threat actors, as well as compelling reasons to address those threats.

Given companies' unparalleled visibility into cyberthreats, the government has long encouraged the private sector to work with authorities to identify and address cyber-threats. The

[27] *See* Exec. Order 14028, § 1 (2021).

[28] President's Nat'l Infrastructure Advisory Council, *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, at 3 (Aug. 2017), https://perma.cc/4TNE-8G85.

Cybersecurity Information Sharing Act of 2015[29] provided companies some protections for voluntarily sharing information with the federal government about "cyber threat indicators" and "defensive measures" taken to mitigate an attack.[30] In March 2022, Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022,[31] which requires the Cybersecurity and Infrastructure Security Agency ("CISA") to issue rules about when certain cyber incidents *must* be privately reported to federal authorities and encourages voluntary reporting of others.[32] CISA, FBI, and a host of other government agencies currently invite and enable private-sector partners to report a wide range of cybersecurity issues, from software vulnerabilities to full-scale hacks.[33] Authorities have recognized that close cooperation between the public and private sectors is "vital" for the government to learn about cyber-threats.[34] As FBI Director Christopher Wray explained, "[i]f American businesses don't report attacks and intrusions, we don't know about most of them, which means we can't help [businesses] recover, and we don't know how to stop the next attack."[35]

In addition to encouraging private businesses to report information about cyber issues to law enforcement and national security authorities, the government has also fostered exchanges of

---

[29] 6 U.S.C. § 1501 *et seq.*

[30] *Id.* § 1504(a)(2).

[31] *See id.* § 681 *et seq.*

[32] *Id.* §§ 681b–681c.

[33] CISA, *Report to CISA*, https://perma.cc/5N47-DLYP; *see also* FBI, *Internet Crime Complaint Center (IC3)*, https://perma.cc/6TS9-CAYA ("Nation's central hub for reporting cyber crime"); DHS, *Harmonization of Cyber Incident Reporting to the Federal Government* at B1–53 (Sept. 19, 2023), https://perma.cc/GKL8-B5HC (describing 52 distinct requirements for reporting cyber incidents to federal agencies).

[34] Lisa O. Monaco, Dep. U.S. Att'y Gen., *Op-Ed: America Needs Congress's Help to Solve the Ransomware Threat*, CNBC (Oct. 6, 2021), https://perma.cc/8ZMD-223Z ("[M]uch of what investigators and prosecutors will know about a ransomware or digital extortion attack depends on what victims tell us — and when.").

[35] Christopher Wray, Remarks at the Detroit Economic Club, FBI Partnering With the Private Sector to Counter the Cyber Threat (Mar. 22, 2022), https://perma.cc/B2UA-FNQH .

information among companies about cyber-threats and how they can be mitigated. For example, the White House has encouraged the creation of information-sharing and analysis centers ("ISACs") and information-sharing and analysis organizations ("ISAOs") to gather, analyze, and disseminate information about cyber-threats across industries and other communities of interest.[36] Congress and the Executive Branch have also broadly exempted from antitrust scrutiny bona fide information-sharing among competitors about cybersecurity issues.[37] As a result of these measures, systems for aggregating information about cybersecurity threats are now commonplace.[38]

This case threatens to impede the information-sharing the Executive Branch and Congress have long recognized as essential to effective cyber defense.[39] The SEC effectively seeks to hold Defendants liable in part because SolarWinds allegedly did not disclose specifics about its cybersecurity vulnerabilities or immediately disclose certain details about the SUNBURST incident.[40] And it claims that Defendants were aware of those undisclosed issues based on various communications among SolarWinds employees (or between SolarWinds and third parties). If sustained, the SEC's theory risks stifling the candid communications on which effective cybersecurity relies. Consider, for example, if an engineer became aware of some unsuccessful

---

[36] White House, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (May 22, 1988), https://perma.cc/VK4B-9769 (ISAC); Exec. Order 13691, § 2(a) (2015) (ISAOs). There are now than two dozen ISACs facilitating the exchange of information in different industries. *See* Nat'l Council of ISACs, *Member ISACs*, https://perma.cc/D8MW-MUEN.

[37] 6 U.S.C. § 1503(e); Dep't of Justice & Fed. Trade Comm'n, *Antitrust Policy Statement on Sharing of Cybersecurity Information* (Apr. 10, 2014), https://perma.cc/YH5M-PDDD; Joel I. Klein, Antitrust Div., Dep't of Justice, *Response to Electric Power Research Institute, Inc.'s Request for Business Review Letter* (Oct. 2, 2000), https://perma.cc/9H35-F463.

[38] *See* CISA, *Automated Indicator Sharing (AIS)*, https://perma.cc/5QKQ-QP2B.

[39] *See generally* Br. of Amici Curiae Former Government Officials.

[40] *See supra* pp. 5–6.

efforts to probe his or her employer's cyber-defenses and reported those efforts to the government or shared information about them with other companies in the industry. Particularly if the threat activity ultimately led to a successful attack, the SEC might claim that the company failed to promptly disclose a material risk or event to investors, pointing to the engineer's external communications to establish that the company was aware of that problem yet failed to disclose it.[41]

That risk is both troubling for companies and bad for cybersecurity. To identify and address cyber-threats and incidents, companies must be able to speak freely and openly; cyber-threat information communicated within the organization or shared with law enforcement or external cybersecurity professionals necessarily will be more detailed or technical than what can appropriately be shared with investors. Organizations committed to cybersecurity strive to build and maintain a "see something, say something" security culture in which all employees are encouraged to speak up about potential threats and vulnerabilities.[42] Within organizations, employees must be able to candidly discuss actual or potential cybersecurity issues, both among each other and with management. Once incidents are discovered, cybersecurity professionals do not have the luxury of lengthy time to deliberate, but must act quickly and with limited information in confusing, difficult, and rapidly evolving situations. In that context, companies will often share information as it becomes known, even though the information may be fragmentary and may later

[41] Although the Cybersecurity Information Sharing Act of 2015 limits the purposes for which agencies may use cyber-threat indicators and defensive measures shared under that Act, that limitation is restricted to information sharing "under th[at]" Act and specifically permits information to be used for "a cybersecurity purpose." 6 U.S.C. § 1504(d)(5)(A), (B).

[42] In that same vein, CISA encourages organizations to take affirmative steps to spot vulnerabilities and instill a culture of cybersecurity awareness across the workforce. *See* CISA, *Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness* (2021), https://perma.cc/7SX7-WA5T; CISA, Blog, *Questions Every CEO Should Ask About Cyber Risks* (Feb. 1, 2021), https://perma.cc/R6KY-NCBS .

turn out to be incorrect. Such prompt information-sharing is essential to protecting customers, helping other companies avoid the same problems, and assisting the government in remedying the issue.[43]

But that prompt, candid information-sharing will be chilled if companies fear that the SEC may scour their communications for evidence about what the company knew about cybersecurity issues and whether and when they disclosed the same information to their investors. If companies fear that candid internal communications among engineers and other employees will be taken as evidence that those companies knew about cybersecurity vulnerabilities but did not disclose them to investors, companies may try to avoid documenting those concerns. Moreover, if companies have reason to believe that information they share with law enforcement authorities will similarly be turned against them, they may be more reluctant to share detailed, actionable information; some could even be forced to withdraw from voluntary reporting entirely.[44]

In response to concerns that the government had adopted too "confrontational" a posture towards private industry following previous cybersecurity incidents,[45] FBI Director Wray underscored that his agency was "laser-focused on the bad guys" and was "not asking [companies] for information so [they] can turn around and share it with regulators looking into the adequacy of

[43] *See* Monaco, *supra* note 34.

[44] Moreover, as the brief of amici curiae Chief Information Security Officers and Cybersecurity Organizations explain, the SEC's attempts to hold SolarWinds' chief information security officer individually liable will also likely inhibit individual cybersecurity employees from communicating about these issues and to hamper companies' ability to recruit these employees.

[45] Eugenia Lostri et al, CSIS, *A Shared Responsibility: Public-Private Cooperation for Cybersecurity*, at 6 (Mar. 2022), https://perma.cc/7AMW-B2CK (discussing how the FTC threatened legal action against some companies that supposedly took too long to patch their systems following discovery of a zero-day vulnerability in the Log4j Java logging system).

[companies'] cybersecurity after a breach."[46] But that is effectively what will happen if the SEC pursues enforcement actions against cyberattack victims and their employees based on information those companies voluntarily submitted to the government or shared with other companies.[47]

B. This Case Will Limit Companies' Ability to Communicate with Customers and the Public About Emerging Cyberthreats.

This case threatens to chill companies' communications about cybersecurity not only with the government and other companies, but also with customers and the public. Companies with active cybersecurity platforms routinely communicate with customers and the public through update alerts and blogs. The content and intended audience of these communications vary. Some provide basic cybersecurity information useful to any potentially affected user or organization. Others provide advanced, technical information about threat signals and other indicators of compromise, which are intended for cybersecurity professionals charged with safeguarding the systems of their respective organizations.

Regardless of their audience, such communications promote cybersecurity in at least two key ways. *First*, they serve as an important channel for industry participants to share best practices and knowledge about current cyber-threats, which not only helps educate companies about cybersecurity but, in so doing, makes all users safer by promoting a more secure digital ecosystem.

---

[46] Christopher Wray, Remarks at the Economic Club, Working With Our Private Sector Partners to Combat the Cyber Threat (Oct. 28, 2021), https://perma.cc/KR3L-XQDN.

[47] The SEC takes a broad view of its investigative authority to compel victims of cyber-attacks to disclose sensitive contemporaneous communications about those attacks, despite the chilling effect such measures may have on victims' cooperation with law enforcement. *See* Mem. Op., *SEC v. Covington & Burling, LLP*, No. 1:23-mc-00002-APM, ECF 42 (D.D.C. July 24, 2023) (partially enforcing SEC subpoena seeking disclosure of law firm clients whose data was potentially compromised in state-sponsored cyber-attack perpetrated against law firm); *id.* at 18 (observing that SEC's investigative tactics "could cause [victim] companies who experience cyberattacks to think twice before seeking legal advice from outside counsel" and that victim law firms "very well might hesitate to report cyberattacks to avoid scrutiny of their clients").

Second, these communications also deter bad actors and thereby reduce the incidence of future cyberattacks. When attacks are publicized, threat actors will often abandon their existing tactics, techniques, and procedures, and shift to new ones, requiring them to expend additional resources. Moreover, companies often use blogs and other public communications to attribute responsibility for particular attacks to specific threat actors. Such "naming and shaming" by companies supports U.S. government efforts to put pressure on nation-state and state-backed threat actors.[48]

The SEC's suit imperils companies' ability to continue these important communications. For the reasons discussed above, companies may be reluctant to publish information about potential threats if the SEC will later mine those publications for evidence that the companies were aware of threats they did not specifically reference in their SEC filings. And companies may be especially uneasy maintaining blogs, issuing customer alerts, and making other similar industry communications about the rapidly evolving cyber-threat landscape if they fear that the SEC will pluck language from them to argue that these companies were downplaying risks or overstating their own capabilities. That is in essence what the SEC has done to Defendants in this case.

The SEC dedicates much of its complaint to allegations that SolarWinds exaggerated its cybersecurity capabilities in a "Security Statement" posted on the company's website but not included in its SEC filings.[49] The SEC attempts to pick that Statement apart, arguing that certain general claims made in the Statement about the company's security policies were materially false

[48] *See* White House, National Cybersecurity Strategy at 32 (Mar. 2023), https://perma.cc/P6VJ-B4FF (discussing role of "coordinated statements of attribution" in conveying "simultaneous diplomatic condemnation of many governments and strengthening the coalition committed to a stable cyberspace").

[49] Defs.' Mot. to Dismiss (ECF 46) at 20–26.

or misleading because the company is alleged to have sometimes not lived up to those policies.[50] But there is no reason why that logic would not also extend to companies' security alerts, blogs, or other public-facing communications—for example, a post notifying customers that a threat has been detected and mitigated. Under the SEC's theory, the company would face an increased risk of being sued for securities fraud if those mitigation measures ultimately proved inadequate.

In short, the effect of this suit will thus be not only to hamper efforts to detect and remediate cyber problems, but also to chill an important source of public information about cybersecurity, to the detriment of the global information technology ecosystem.

CONCLUSION

Defendants' motion to dismiss should be granted.

Dated: February 2, 2024

Respectfully submitted,

/s/ James M. Garland

James M. Garland (*pro hac vice* pending)
Megan A. Crowley (*pro hac vice* pending)
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
(202) 662-6000
jgarland@cov.com
mcrowley@cov.com

S. Conrad Scott
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018
(212) 841-1249
cscott@cov.com

Counsel for BSA | The Software Alliance

[50] *See* Compl. ¶¶ 47–52 (alleging that claim to follow NIST Standards was false because company scored itself poorly on assessment); *id.* ¶¶ 58–68 (alleging that claim to follow secure development lifecycle was false because company "did not always" do so); *id.* ¶¶ 73–84 (alleging that claim to have strong password policy was false because company "failed to enforce or comply with its own password policy on multiple occasions" (capitalization altered)); *id.* ¶¶ 88–100 (claim to have access controls was false because company's access controls were allegedly "poor").